



U.S. Army Cyber Command

October is Cyber Security Awareness Month – When using the internet, remember to “Stop, Think and Connect”

The Environment

- The Threat is Real, Active & Growing.
- Army Networks, Soldiers and Families are targets in Cyberspace.
- Success in cyber operations is a team sport – we depend on your awareness of the cyber threat.



Leader's Responsibilities

- Cyber Security is a Command Responsibility.
- Responsible for Soldier's actions on the network – enforce standards!
- Compliance with Information Assurance (IA) standards and discipline.
- Process only information at the highest level authorized for that system.
- Protect DoD networks – Garrison, Expeditionary, Coalition.
- Integration of Cyber planning into the staff process (2-3-6).
- Train teams on incident reporting and response.
- Maintain critical network infrastructure in garrison and tactical environments.
- Plan and support Network Integration Exercises before deployments to CTCs and combat operations.

Helpful links :

- Free anti virus for home use:
https://www.acert.1stiocmd.army.mil/Antivirus/Home_Use.htm
- Army Cyber Command:
<http://arcyber.army.mil/cyber-awareness.html>
- Internet Crime Complaint Center (IC3):
<http://www.ic3.gov/default.aspx>
- Identity theft reporting to the Federal Trade Commission:
<http://www.ftc.gov/idtheft>

Soldier's Responsibilities

- You are accountable for your actions.
- Individual training and cyber awareness (Annual Cyber Security Awareness training).
- OPSEC – protect critical information.
- Protect Army networks from:
 - Phishing attacks.
 - Cross-domain violations.
 - Unauthorized disclosures of classified information.
- Ensure that you:
 - Do not connect unauthorized hardware to DoD networks (iPod, flash drives, cameras).
 - Do not install unauthorized software on DoD networks (Peer-to-peer, key loggers).
 - Report suspected violations to your chain of command immediately.
- At home:
 - Free antivirus support is available for home use.
 - Social Media – NEVER disclose personal information on social networking sites.
 - Click with caution when following links in emails or on social networking sites.
 - Hide your profile from search engines.
- Mobile:
 - Know your Apps – protect your personal information.
 - Protect your device from theft – report criminal acts to the authorities.